

A Critical Look at Self-Dual Codes*

Judy L. Walker

Department of Mathematics and Statistics
University of Nebraska
Lincoln, NE 68588-0323
jwalker@math.unl.edu

Abstract

We investigate self-dual codes from a structural point of view. In particular, we study properties of critical indecomposable codes which appear in the spectrum of a self-dual code. As an application of the results we obtain, we revisit the study of self-dual codes of dimension at most 10.

1 Introduction

In the late 1950's, Slepian [4] became the first to take an abstract approach to the study of error-correcting codes. He introduced a structure theory for binary linear codes, developing in particular the idea of an *indecomposable code*; that is, a code which is not isomorphic to a nontrivial direct sum of two other codes. He proved two important results in this direction: First, every code is isomorphic to a unique sum of indecomposable codes. Second, for a given length and dimension, there is an indecomposable code which achieves the highest possible minimum distance.

The problem with indecomposable codes is that there are simply too many of them. A code is indecomposable if and only if it is not equivalent to a code which has a generator matrix which is block diagonal with at least two blocks. Thus, if C is any indecomposable code, then adding any column onto C yields a new indecomposable code of the same dimension but length one more than the length of C .

The major breakthrough in this area came in the late 1990's when Assmus ([1]) introduced the notion of *critical indecomposable* codes. The idea is that these codes are indecomposable codes with no "extra" columns tacked on. The notion of critical indecomposable codes appears to be very promising. In fact, Assmus shows that there is a "quasi-canonical" form for the generator matrix of such a code. Further, Assmus gives a recursive construction for all critical indecomposable codes.

A critical indecomposable code which can be obtained by puncturing an indecomposable code at one or more columns is said to be in the *spectrum* of that indecomposable code. In this paper, we investigate self-dual codes by considering properties of critical indecomposable codes which appear in the spectrum of a self-dual code. Recall that a code $C \subset \mathbb{F}_q^n$ is called *self-dual* if $C = C^\perp$, where $C^\perp := \{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for every } c \in C\}$. These codes are known to have many remarkable properties, and much work has been done toward understanding them. In particular, considerable effort has been devoted to

*This research is supported in part by NSF Grants DMS-0071008 and DMS-0071011.

finding a complete enumeration of self-dual binary codes. Though the enumeration is now known through dimensions at least 16, the first paper on the subject ([3]) dealt with self-dual codes of dimension at most 10, a topic we revisit in this paper.

2 Critical Indecomposable Codes

We begin by recalling some definitions and results from [1] and [5]. In what follows, all codes are assumed to be binary, and we will write \mathbb{F} to mean the field with two elements.

Definition 2.1. Let C' and C'' be linear codes of lengths m and n respectively. The *direct sum* of C' and C'' is the set $C := C' \oplus C''$ of all vectors $\mathbf{c} = (c_1, \dots, c_{m+n}) \in \mathbb{F}^{m+n}$ such that $(c_1, \dots, c_m) \in C'$ and $(c_{m+1}, \dots, c_{m+n}) \in C''$. Two codes are *isomorphic* if one can be obtained from the other through a permutation of coordinates. A code C is called *indecomposable* if it is not isomorphic to $C' \oplus C''$ for any nonzero linear codes C' and C'' . A code which is not indecomposable is called *decomposable*.

Let C be an indecomposable code of length n and dimension k and let G be a generator matrix for C . For $1 \leq i \leq n$, define $\phi_i(C)$ to be the code which is generated by the rows of the matrix obtained from G by omitting the i th column. (This process is known as *puncturing* C at the i th column and is clearly independent of the choice of the generator matrix for C .) Then $\phi_i(C)$ will be a code of length $n - 1$ and dimension either k or $k - 1$, and it may or may not be indecomposable.

Definition 2.2. Let C be an indecomposable code of length n . We say the i th column of C is a *critical column* of C if either $\phi_i(C)$ has dimension $k - 1$ or $\phi_i(C)$ is decomposable. We say C is a *critical indecomposable code* if every column of C is critical.

It is plain to see that \mathbb{F} is the only critical indecomposable code of dimension 1. Further, for $k \geq 2$, there is only one code of dimension k and length $k + 1$, and it is critical indecomposable. We will call this code $C_{k+1,k}$. There is also (see [5]) a unique critical indecomposable code $C_{2k-2,k}$ of length $2k - 2$ and dimension k for each $k \geq 4$, and this is the longest critical indecomposable code of dimension k . Moreover, Assmus gives a recursive construction for all critical indecomposable codes.

The construction takes as input a partition $\pi = (x_1, \dots, x_r, x')$ of the intended length n of the code and an *auxiliary code* A , which is indecomposable of length $s := r + x'$ and minimum distance at least 3. We require that $x_i \geq 2$ for $i = 1, \dots, r$, and we assume without loss of generality that it is ordered so that $x_1 \geq x_2 \geq \dots \geq x_r$. Further, we require that the last x' columns of A be critical. Then a generator matrix for a critical indecomposable code can be constructed from π and A as follows:

- For $1 \leq i \leq r$, let G_i be the $(x_i - 1) \times x_i$ matrix which consists of a column of 1's followed by the identity matrix of size $x_i - 1$. Note that if $x_i = 2$, then G_i is a generator matrix for the code whose only nonzero element is the vector $(1, 1)$; otherwise G_i generates the code $C_{x_i, x_i - 1}$ described above.
- Let $l = \dim A$ and fix a generator matrix G_A for A . For $1 \leq i \leq r$, let L_i be the $l \times x_i$ matrix whose first column is the i th column of G_A and whose other entries are all 0. Also let $L_{r+1}, \dots, L_{r+x'}$ be the last x' columns of G_A .

- Set

$$G := \begin{pmatrix} G_1 & & & & & & \\ & \ddots & & & & & \\ & & G_r & & & & \\ L_1 & \dots & L_r & L_{r+1} & \dots & L_{r+x'} & \end{pmatrix}, \quad (*)$$

where all blank spaces are assumed to be filled in with zeros.

The matrix G is a generator matrix for a critical indecomposable code of length n and dimension $k := n - s + l$. The relatively straight-forward proof is given in [1], and we will not reproduce it here. A generator matrix of this form is called *quasi-canonical* because the first $k - l$ rows are uniquely determined by π and the last l are determined by A .

It is also true (see [1] or [5]) that every critical indecomposable code is equivalent to a code with a generator matrix of the form $(*)$, and from this generator matrix, we may recover a partition and auxiliary code. Thus, given any critical indecomposable code C , it makes sense to refer to the partition and auxiliary code used to construct C .

In [5], we give a complete enumeration of critical indecomposable codes of dimension at most 10. This enumeration is given in terms of the partitions and auxiliary codes used in the constructions.

Finally, we present some notational conventions used in the remainder of the paper. For a matrix M , we will write M^t for the transpose of M . We will write $(\mathbf{w}_1 | \mathbf{w}_2)$ to mean the vector formed by concatenating the vectors \mathbf{w}_1 and \mathbf{w}_2 . If D is an indecomposable code, we will write $\text{Spec}(D)$ for the *spectrum* of D , i.e., the set of critical indecomposable codes which can be obtained by puncturing D at one or more columns. Also, we will often blur the distinction between equivalent codes. For example, when $C \in \text{Spec}(D)$, we will say that D has a generator matrix of the form $[G|M]$ where G is a generator matrix for C , rather than that D is equivalent to a code with a generator matrix of this form.

3 Applications to Self-Dual Codes

We begin with some results about critical indecomposable codes with lengths at the two extremes of the range of possibilities.

Theorem 3.1. *For each $k \geq 4$, the unique critical indecomposable code $C_{2k-2,k}$ of length $2k - 2$ and dimension k is in the spectrum of a self-dual code if and only if k is even. Further, when k is even, there is a unique self-dual code D with $C_{2k-2,k} \in \text{Spec}(D)$ and D is doubly-even (i.e., all words in D have weight divisible by 4) if and only if $k \equiv 0 \pmod{4}$.*

Proof. The quasi-canonical generator matrix for the code $C_{2k-2,k}$ is

$$G := \begin{pmatrix} 11 & & & & \\ & \ddots & & & \\ & & & 11 & \\ 10 & \dots & & 10 & \end{pmatrix},$$

so if D is a self-dual code with $C_{2k-2,k} \in \text{Spec}(D)$, then D must have a generator matrix of the form $[G|M]$, where M is a $k \times 2$ matrix with rows m_1, \dots, m_k . If k is odd,

then all rows of G have even weight; thus all rows of M must have even weight, but we also must have $m_i \cdot m_k = 1$ for $1 \leq i \leq k - 1$ and this is impossible. If k is even, the only possibility for the rows of M is $m_i = (1, 1)$ for $1 \leq i \leq k - 1$ and (without loss of generality) $m_k = (1, 0)$. Finally, we see that the rows of $[G|M]$ all have weight divisible by 4 if and only if $k \equiv 0 \pmod{4}$, which completes the proof of the theorem. \square

Our next task is to show that no critical indecomposable code of dimension k and length $k + 1$ can appear in the spectrum of a self-dual code. First we prove a lemma which will be used both in the proof of this statement and later in the paper.

Lemma 3.2. *Let M be a $r \times c$ matrix and set $S := MM^t$. Then the rank of S is at most c . Further, if every row of M has even weight, then the rank of S is at most $c - 1$.*

Proof. The matrix S represents the composition $\mathbb{F}^r \rightarrow \mathbb{F}^c \rightarrow \mathbb{F}^r$, where the map $\mathbb{F}^r \rightarrow \mathbb{F}^c$ is given by M^t and the map $\mathbb{F}^c \rightarrow \mathbb{F}^r$ is given by M . Therefore, the rank of S is at most the column rank of M , which is at most c . If every row of M has even weight, then $(1, \dots, 1)^t$ is in the null space of M . Thus, in this case the column rank of M is at most $c - 1$. \square

Theorem 3.3. *For any $k \geq 2$, the unique critical indecomposable code $C_{k+1,k}$ of length $k + 1$ and dimension k is not in the spectrum of any self-dual code.*

Proof. Suppose $C_{k+1,k} \in \text{Spec}(D)$ for some self-dual code D . Then D has a generator matrix of the form $[1|I|M]$, where every row of the $k \times (k - 1)$ matrix M has even weight and the inner product of any two distinct rows of M is 1. The matrix MM^t is then the $k \times k$ matrix which has 0's on the diagonal and 1's elsewhere. Such a matrix has rank either k or $k - 1$ depending on whether k is even or odd. However, by Lemma 3.2, the rank of MM^t is at most $k - 2$. This shows that M , and hence D , cannot exist. \square

In studying which of the other critical indecomposable codes can appear in the spectrum of a self-dual code, we will find the next definition useful.

Definition 3.4. Let $\pi := (x_1, \dots, x_r, x')$ be a partition of the integer n and set $s := r + x'$. The maps $i_\pi : \mathbb{F}^s \rightarrow \mathbb{F}^n$ and $j_\pi : \mathbb{F}^s \rightarrow \mathbb{F}^n$ are defined by $i_\pi(a_1, \dots, a_s) := (a_1^{x_1}, \dots, a_r^{x_r}, a_{r+1}, \dots, a_s)$ and $j_\pi(a_1, \dots, a_s) := (a_1, 0^{x_1-1}, \dots, a_r, 0^{x_r}, a_{r+1}, \dots, a_s)$, where a^x is the vector of length x all of whose entries are a .

Lemma 3.5. [1] *Let C be a critical indecomposable code. Let π be the partition and let A be the auxiliary code used in the construction of C . Then $C^\perp = i_\pi(A^\perp)$.*

Proof. Let n be the length of C , k the dimension of C , s the length of A , and l the dimension of A . Then $n - k = s - l$, which means that $\dim(C^\perp) = \dim(A^\perp) = \dim(i_\pi(A^\perp))$. Thus, it is enough to show that $i_\pi(\mathbf{b}) \cdot \mathbf{f} = 0$ for every $\mathbf{b} \in A^\perp$ and every row \mathbf{f} in a quasi-canonical generator matrix for C . Let $\mathbf{b} = (b_1, \dots, b_s) \in A^\perp$. If \mathbf{f} is one of the first $k - l$ rows of a quasi-canonical generator matrix for C , then \mathbf{f} has weight 2 and support contained entirely within the block corresponding to some x_i , $1 \leq i \leq r$, where $\pi = (x_1, \dots, x_r, x')$. Thus $i_\pi(\mathbf{b}) \cdot \mathbf{f} = b_i + b_i = 0$. On the other hand, if \mathbf{f} is one of the last l rows, then $\mathbf{f} = j_\pi(\mathbf{a})$ for some $\mathbf{a} \in A$. Thus $i_\pi(\mathbf{b}) \cdot \mathbf{f} = 0$ since $\mathbf{b} \in A^\perp$. \square

Theorem 3.6. *Let C be a critical indecomposable code and suppose that C is in the spectrum of some self-dual code. Then $C^\perp \subseteq C$.*

Proof. Let D be a self-dual code with $C \in \text{Spec}(D)$. Let n and k be the length and dimension of C so that D has length $2k$. We may assume that C is obtained by puncturing D at the last $2k - n$ columns. Let $\mathbf{z} = (z_1, \dots, z_n) \in C^\perp$ and let $\mathbf{y} = (y_1, \dots, y_{2k})$ be the vector of length $2k$ such that $y_i = z_i$ for $1 \leq i \leq n$ and $y_i = 0$ for $n + 1 \leq i \leq 2k$. Let $\mathbf{d} = (d_1, \dots, d_{2k})$ be any codeword in D . Then $\mathbf{y} \cdot \mathbf{d} = \sum y_i d_i = \sum z_i d_i = 0$ since $(d_1, \dots, d_n) \in C$. Hence $\mathbf{y} \in D^\perp = D$, and so $\mathbf{z} \in C$. \square

This theorem turns out to be quite powerful and will severely restrict which critical indecomposable codes can appear in the spectrum of a self-dual code. The crucial step in obtaining this restriction is given by the next lemma.

Lemma 3.7. *Let C be the critical indecomposable code constructed from the partition $\pi = (x_1, \dots, x_r, x')$ and the auxiliary code A , and suppose C is in the spectrum of some self-dual code. Let \mathbf{b} be any codeword of A^\perp . If the only codeword of A with support contained in $\text{supp}(\mathbf{b})$ is 0, then $\text{supp}(\mathbf{b}) \subset \{1, \dots, r\}$ and x_i is even for every $i \in \text{supp}(\mathbf{b})$. If $\text{supp}(\mathbf{b}) \not\subset \{1, \dots, r\}$, then there is a codeword $\mathbf{a} \in A$ with $\text{supp}(\mathbf{b}) \setminus \{1, \dots, r\} \subset \text{supp}(\mathbf{a}) \subset \text{supp}(\mathbf{b})$.*

Proof. Let $\mathbf{b} \in A^\perp$. Then $i_\pi(\mathbf{b}) \in C$, and so $i_\pi(\mathbf{b}) = \mathbf{e} + j_\pi(\mathbf{a})$ for some $\mathbf{e} := (\mathbf{e}_1 | \dots | \mathbf{e}_r) \in E_1 \oplus \dots \oplus E_r$ and some $\mathbf{a} := (a_1, \dots, a_r, a_{r+1}, \dots, a_{r+x'}) \in A$. For $r+1 \leq i \leq r+x'$, we see that $b_i = a_i$, so the supports of \mathbf{b} and \mathbf{a} are identical in the last x' columns. For $1 \leq i \leq r$, if $a_i = 1$, then $b_i = 1$ since E_i has minimum distance 2. Thus, $\text{supp}(\mathbf{a}) \subset \text{supp}(\mathbf{b})$. In particular, if 0 is the only codeword of A with support contained in $\text{supp}(\mathbf{b})$, then the last x' coordinates of \mathbf{b} must be zero. Further, in that case, we must have the all-one vector contained in E_i for each $i \in \text{supp}(\mathbf{b})$, which implies that x_i must be even for all $i \in \text{supp}(\mathbf{b})$. \square

We now use this lemma to find necessary conditions on the ingredients used to construct a critical indecomposable code which appears in the spectrum of a self-dual code.

Theorem 3.8. *Let $C = C(\pi, A)$ be the critical indecomposable code constructed using the partition $\pi = (x_1, \dots, x_r, x')$ and the auxiliary code A , where the dimension of C is at most 10. If C is in the spectrum of a self-dual code, then $x' = 0$ and each x_i is even.*

Proof. All critical indecomposable codes of dimension at most 10 are listed in [5] according to the partitions and auxiliary codes used to construct them. The idea of this proof is to consider each auxiliary code in turn. To set up notation, let $s := r + x'$ and l be the length and dimension of the auxiliary code A .

If $l = 1$, then $A = A_{s,1}$ for some s and $A^\perp = C_{s,s-1}$. Since A has no critical columns, we already have $x' = 0$ and $r = s$. Further, since $i_\pi(A^\perp) = C^\perp \subseteq C$ by Lemma 3.5 and Theorem 3.6, we have that $i_\pi(\mathbf{f}_i) \in C$ where \mathbf{f}_i is the i th row of the generator matrix $[I|1]$ for $C_{s,s-1}$. But $\text{supp}(i_\pi(\mathbf{f}_i))$ is the set of coordinates in the blocks corresponding to x_i and x_s . This means that x_i and x_s are even by Lemma 3.7. Since $\mathbf{f}_i \in C_{s,s-1}$ for $1 \leq i \leq s-1$, we have that x_j is even for all j .

Now suppose $l = 2$. The shortest admissible code of dimension 2 has length 5, and so we have $s \geq 5$. Without loss of generality we may assume that the three nonzero codewords of A are $(1^u, 0^v, 1^w)$, $(0^u, 1^v, 1^w)$, and $(1^u, 1^v, 0^w)$ where u , v , and w satisfy $u \geq 2$, $v \geq 2$, and $u + v + w = s$. Let $u_0 = 2\lfloor u/2 \rfloor$, so that u_0 is the largest even integer which is not larger than u . Then $(1^{u_0}, 0^{u-u_0}, 0^v, 0^w) \in A^\perp$ and by Lemma 3.7, x_1, \dots, x_{u_0} must all be even. Since the vector $(0^{u-2}, 1^2, 0^v, 0^2)$ is also in A^\perp , we get that x_{u-1} and x_u are both even. Likewise, we can show that x_{u+1}, \dots, x_{u+v} are all even. If

$x' = 0$, a similar argument (using the vector $(1, 0^{u-1}, 1, 0^{v-1}, 1^w)$ if w is odd, or the vectors $(1, 0^{u-1}, 1, 0^{v-1}, 1^{w-1}, 0)$ and $(1, 0^{u-1}, 1, 0^{v-1}, 0, 1^{w-1})$ if w is even) shows that $x_{u+v+1}, \dots, x_{u+v+w}$ are all even. In summary, when $l = 2$ and $x' = 0$, each x_i must be even.

If $l = 2$ and $x' = 1$, then A must have a critical column, which we may assume is the last column of A . This means, in particular, that $w = 1$ in this situation. Then $(1, 0^{u-1}, 1, 0^{v-1}, 1) \in A^\perp$, and so by Lemma 3.7, we must have a vector $\mathbf{a} \in A$ with $1 \in \text{supp}(\mathbf{a}) \subset \{1, u+1, s\}$. Such an \mathbf{a} does not exist, and so x' must be 0.

Next, suppose $l = 3$. There is no nice general description of the nonzero codewords in admissible codes of dimension 3. However, we still use the basic idea of finding explicit codewords in the dual code and applying Lemma 3.7. For example, consider the admissible code $A_{7,3,1}$, which has quasi-canonical generator matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

One sees immediately that $(1, 1, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 0, 0, 0)$, and $(0, 0, 0, 0, 1, 1, 0)$ are all in $A_{7,3,1}^\perp$, and applying Lemma 3.7, we find that any partition used with $A_{7,3,1}$ must have x_i even for $1 \leq i \leq 6$. Taking any word of $A_{7,3,1}^\perp$ supported on the last column (for example, $(1, 0, 1, 0, 0, 1, 1)$), we find that x' must be 0 and x_7 must be even as well.

The arguments for the rest of the admissible codes are the same, using the codewords in the dual codes supplied by the following table.

A	relevant words in A^\perp
$A_{6,3,0}$	$(0, 1, 0, 1, 1, 0)$, $(1, 1, 0, 0, 0, 1)$, and $(0, 0, 1, 1, 0, 1)$
$A_{7,3,0}^1$	$(0, 1, 0, 1, 1, 0, 0)$, $(1, 1, 0, 0, 0, 1, 0)$, $(0, 0, 1, 1, 0, 1, 0)$, and $(1, 0, 0, 0, 0, 0, 1)$
$A_{7,3,0}^2$	$(0, 1, 0, 1, 1, 0, 0)$, $(1, 1, 0, 0, 0, 1, 0)$, $(0, 0, 1, 1, 0, 1, 0)$, and $(1, 0, 0, 1, 0, 0, 1)$
$A_{8,3,1}^1$	$(1, 1, 0, 0, 0, 0, 0, 0)$, $(0, 1, 1, 0, 0, 0, 0, 0)$, $(0, 0, 0, 1, 1, 0, 0, 0)$, $(0, 0, 0, 0, 0, 1, 1, 0)$, and $(1, 0, 0, 0, 1, 0, 1, 1)$
$A_{8,3,1}^2$	$(1, 1, 0, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 0, 0, 0, 0)$, $(0, 0, 0, 0, 1, 1, 0, 0)$, $(1, 0, 0, 0, 0, 1, 1, 0)$, and $(0, 0, 1, 0, 0, 0, 1, 1)$
$A_{7,3,2}$	$(1, 1, 0, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 0, 0, 0, 0)$, $(0, 0, 0, 1, 1, 1, 0)$, and $(1, 0, 0, 0, 1, 0, 1)$
$A_{8,3,2}^1$	$(1, 1, 0, 0, 0, 0, 0, 0)$, $(0, 1, 1, 0, 0, 0, 0, 0)$, $(0, 0, 0, 1, 1, 0, 0, 0)$, $(0, 0, 0, 1, 0, 1, 0, 1)$, and $(1, 0, 0, 0, 0, 1, 1, 0)$
$A_{8,3,2}^2$	$(1, 1, 0, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 0, 0, 0, 0)$, $(0, 0, 0, 0, 1, 1, 0, 0)$, and $(0, 1, 1, 0, 0, 0, 1, 1)$
$A_{9,3,2}^1$	$(1, 1, 0, 0, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 0, 0, 0, 0, 0)$, $(0, 0, 0, 0, 1, 1, 0, 0, 0)$, $(1, 0, 0, 0, 0, 0, 1, 1, 0)$, and $(0, 0, 0, 0, 1, 0, 1, 0, 1)$
$A_{9,3,2}^2$	$(1, 1, 0, 0, 0, 0, 0, 0, 0)$, $(0, 1, 1, 0, 0, 0, 0, 0, 0)$, $(0, 0, 0, 1, 1, 0, 0, 0, 0)$, $(0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$, $(1, 0, 0, 0, 0, 0, 1, 1, 0)$, and $(0, 0, 0, 1, 0, 0, 1, 0, 1)$
$A_{9,3,2}^3$	$(1, 1, 0, 0, 0, 0, 0, 0, 0)$, $(0, 1, 1, 0, 0, 0, 0, 0, 0)$, $(0, 0, 0, 1, 1, 0, 0, 0, 0)$, $(0, 0, 0, 0, 0, 1, 1, 0, 0)$, and $(0, 0, 1, 1, 0, 0, 0, 1, 1)$
$A_{9,3,2}^4$	$(1, 1, 0, 0, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 0, 0, 0, 0, 0)$, $(0, 0, 0, 0, 1, 1, 0, 0, 0)$, $(0, 0, 0, 0, 0, 1, 1, 0, 0)$, and $(0, 1, 1, 0, 0, 0, 0, 1, 1)$
$A_{9,4,3}^1$	$(1, 1, 0, 0, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 0, 0, 0, 0, 0)$, $(0, 0, 0, 0, 1, 1, 0, 1, 0)$, and $(0, 1, 1, 0, 0, 0, 1, 1, 1)$
$A_{9,4,3}^2$	$(1, 1, 0, 0, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 0, 0, 0, 0, 0)$, $(0, 0, 0, 0, 1, 1, 0, 0, 0)$, and $(0, 0, 0, 0, 0, 0, 1, 1, 1)$

□

4 Self-Dual Codes of Dimension At Most 10

In this section, we apply the results obtained above to revisit the enumeration of self-dual codes of dimension at most 10 given by Pless ([3]). It is hoped that these examples will demonstrate how one might hope to obtain new results in larger dimensions using these techniques. As before, we refer to auxiliary codes using the notations of [5].

We treat each dimension $k \leq 10$ in turn. The first five dimensions are easy: When $k = 1$, the code D_2 with generator matrix $[1, 1]$ is the unique self-dual code of dimension 1. When $k = 2$ or 3, the only critical indecomposable code is $C_{k+1,k}$, and so there are no indecomposable self-dual codes in these dimensions by Theorem 3.3. When $k = 4$, there are two critical indecomposable codes: $C_{5,4}$ and $C_{6,4}$. We know $C_{5,4}$ is not in the spectrum of any indecomposable self-dual code by Theorem 3.3, and by Theorem 3.1, $C_{6,4}$ is in the spectrum of a unique indecomposable self-dual code which we will call D_8 . By the same theorem, we know that D_8 is in fact doubly-even. By Theorems 3.3, 3.7, and 3.1, we see that none of the three critical indecomposable codes of dimension 5 can be in the spectrum of any self-dual code, and so there are no indecomposable self-dual codes of dimension 5.

The case where $k = 6$ requires a bit more thought. By Theorem 3.8, the only critical indecomposable codes which might appear in the spectrum of an indecomposable code of dimension 6 are $C((4, 2^2), A_{3,1})$ and $C((2^5), A_{5,1})$, and by Theorem 3.1, this latter code is in the spectrum of a unique self-dual code which we can call D_{12} . In fact, this is the only indecomposable self-dual code of dimension 6. Indeed, any other one must have $C((4, 2^2), A_{3,1})$ in its spectrum. This means it would have a generator matrix of the form $[G|M]$ where G is the quasi-canonical generator matrix for $C((4, 2^2), A_{3,1})$ and M is a 6×4 matrix, chosen carefully so that each pair of rows of $[G|M]$ has inner product 0. Without loss of generality, then, M must be either

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}^t \quad \text{or} \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}^t.$$

In either case, one gets a code equivalent to D_{12} .

For $k = 7$, we have that the only critical indecomposable codes which might appear in the spectrum of a self-dual code are $C_1 := C((4, 2^3), A_{4,1})$ and $C_2 := C((2^5), A_{5,2;1})$ by Theorems 3.8 and 3.1. Suppose first that C_1 is in the spectrum of a self-dual code. Then that self-dual code has a generator matrix of the form $[G|M]$ where G is the quasi-canonical generator matrix for C_1 and M is a 7×4 matrix satisfying

$$MM^t = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

By Lemma 3.2, the matrix MM^t must have rank at most 3, but a quick check shows that this matrix has rank 4. Thus C_1 cannot appear in the spectrum of any self-dual code. On the other hand, it is not hard to see that C_2 is in the spectrum of a unique

self-dual code: any such code must have a generator matrix of the form $[G|M]$, where G is the quasi-canonical generator matrix for C_2 and the only possible choice for M (up to equivalence) is

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}^t.$$

We write D_{14} for this unique indecomposable self-dual code of dimension 7.

Things are only slightly more complicated for $k = 8$. Theorem 3.8 shows that the only critical indecomposable codes which might appear in the spectrum of a self-dual code are $C_1 := C((6, 2^2), A_{3,1})$, $C_2 := C((4^2, 2), A_{3,1})$, $C_3 := C((4, 2^4), A_{5,1})$, $C_4 := C((2^6), A_{6,2;0})$, $C_5 := C((2^6), A_{6,2;1})$, and $C_6 := C((2^7), A_{7,1})$. Further, Theorem 3.1 shows that C_6 is in the spectrum of a unique (doubly-even) self-dual code D_{16}^1 . We can rule out C_4 using Lemma 3.2 since the generator matrix of a self-dual code having C_4 in its spectrum would be $[G|M]$ where G is a quasi-canonical generator matrix for C_4 and M is a 8×4 matrix all of whose rows have even weight and satisfying

$$MM^t = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

and this matrix has rank 4. It is easy to see that there is a unique self-dual code with C_3 in its spectrum: the generator matrix must be $[G|M]$ where G is the quasi-canonical generator matrix for C_3 and M is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}^t.$$

Further, this code is not equivalent to our code D_{16}^1 , and so we call it D_{16}^2 . At this point, one can use a brute force approach to show that these are the only two indecomposable self-dual codes of dimension 8 by constructing all the different ways that C_1 , C_2 , and C_5 could be extended to self-dual codes. Along the way, we discover that $\text{Spec}(D_{16}^1) = \{C_1, C_6\}$ and $\text{Spec}(D_{16}^2) = \{C_1, C_2, C_3, C_5\}$.

For $k = 9$, we can proceed in a similar fashion. Using Theorems 3.7 and 3.1, we find that $C_1 := C((6, 2^3), A_{4,1})$, $C_2 := C((4^2, 2^2), A_{4,1})$, $C_3 := C((4, 2^4), A_{5,2;1})$, $C_4 := C((4, 2^4), (A_{5,2;1})^{(1,5)})$, $C_5 := C((2^6), A_{6,3;0})$, $C_6 := C((4, 2^5), A_{6,1})$, $C_7 := C((2^7), A_{7,2;0})$, $C_8 := C((2^7), A_{7,2;1}^1)$, and $C_9 := C((2^7), A_{7,2;1}^2)$ are the only critical indecomposable codes which could possibly appear in the spectrum of a self-dual code. Using Lemma 3.2, we can rule out C_1 , C_2 , C_6 , and C_9 . We can construct two inequivalent indecomposable

respectively. Calling the self-dual codes we get D_{20}^3 and D_{20}^4 , we compute their spectra to be $\{C_1, C_2, C_3, C_5, C_6, C_7, C_8, C_9, C_{10}, C_{11}\}$ and $\{C_1, C_2, C_3, C_4, C_7, C_8, C_{10}, C_{11}, C_{13}, C_{15}\}$ respectively. By the mass formula, there are still more indecomposable self-dual codes of dimension 10. At this point, we must use brute force on one of our longer critical indecomposable codes. Trying C_{11} , we see that the only possible ways to extend this code to a self-dual code are to add one of the following matrices:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & \bar{x} & x+y \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & x & \overline{x+y} \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & x & 1 & y+z \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & x & 0 & \overline{y+z} \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & y & z & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & y & z & 0 \end{pmatrix}^t, \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & x & z \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & \bar{x} & \bar{z} \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & y & \bar{x} \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & y & \bar{x} \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \overline{x+y} & \overline{x+z} \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & x+y & \overline{x+z} \end{pmatrix}^t,$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & \overline{x+y} & x \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & \overline{x+y} & \bar{x} \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & x & 1 & z \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & x & 0 & \bar{z} \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & y & 1 & z \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & y & 0 & z \end{pmatrix}^t, \text{ or } \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & \bar{y} & x \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & y & x \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & x & z & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & x & z & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & y & 1 & z \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & y & 0 & x+z \end{pmatrix}^t,$$

where x , y , and z can be 0 or 1, and \bar{a} means $1+a$. With the first or third of these matrices, we get D_{20}^3 no matter what choices we make for x , y , and z . We also get D_{20}^3 when $x=0$ with the second matrix (independent of y and z), and we get D_{20}^4 when $x=z$ (independent of y) with the fourth matrix. However, when we use the second matrix with $x=1$, we get a new code which we call D_{20}^5 , and when we use the fourth matrix with $x \neq z$, we get another one, which we call D_{20}^6 . We can now use the mass formula to show that these are all the possibilities. Finally, we compute $\text{Spec}(D_{20}^5) = \{C_{10}, C_{11}\}$ and $\text{Spec}(D_{20}^6) = \{C_1, C_2, C_3, C_6, C_9, C_{11}\}$.

References

- [1] E. F. Assmus, Jr. The category of linear codes. *IEEE Transactions on Information Theory*, 44:612–629, 1998.
- [2] W. Bosma and J. J. Cannon. *Handbook of Magma Functions*. Sydney, Australia, 1996.
- [3] V. Pless. A classification of self-orthogonal codes over $\text{GF}(2)$. *Discrete Math*, 3:209–246, 1972.
- [4] D. Slepian. Some further theory of group codes. *Bell Syst. Tech. Journal*, 39:1219–1252, 1960.
- [5] J. L. Walker. Constructing critical indecomposable codes. Preprint; May, 2000.